==========

H I P A A L E R T Volume 2 No. 11 September 14, 2001

>> From Phoenix Health Systems...HIPAA Knowledge...HIPAA Solutions <<
> Healthcare IT Consulting & Outsourcing <

==========

HIPAAlert is published monthly in support of the healthcare industry's efforts to work together towards HIPAA security and privacy. Direct subscribers total over 14,000.

Do you have interested associates? They can subscribe free at: http://www.hipaadvisory.com/alert/

IF YOU LIKE HIPAALERT, YOU'LL LOVE HIPAADVISORY.COM! -- Phoenix' comprehensive "HIPAA hub of the Internet" per Modern Healthcare. Visit: http://www.hipaadvisory.com
==========

T H I S I S S U E

==========

1 / F R O M T H E E D I T O R S:

There are times, thankfully infrequent, when it's simply not "business as usual." This is such a time. We'd like to take the next moment or two to address two non-HIPAA topics:

First, the Phoenix staff joins you in expressing our support for victims of this week's tragedy, their families, and those who have worked heroically to rescue and treat survivors.

Second, because HIPAAlert is fortunate to reach such a large IT audience, we felt we should pass on the following request for assistance: The American Red Cross Emergency Operations Centers need donations of a variety of computing and communications equipment, including PCs, laptops, PDAs, hubs, network cards, printers, Zip drives, Nextel cell phones, and more. For a full list and contact info, go to http://www.hipaadvisory.com.

This month's issue reflects new concerns about security, including information security protections of government functions and other critical services -- healthcare, of course, being among them. Our latest news covers Congress'renewed focus

on information sharing and protection, as well as a report on heightened fears of privacy holes that could be created by national security upgrades. In addition, security experts Eric Maiwald and Barry Lyons of Fortrex Technologies offer healthcare organizations a timely prescription for technical security assessment and disaster recovery planning.

With the coming of fall we can expect to see final Security, Provider Identifier and Employer Identifier rules soon, as promised before year end by DHHS. Much is written on HIPAA security, but surprisingly we've seen little discussion of the national identifiers and how they fit into HIPAA planning. So, in this issue, we offer a detailed analysis of the expected final identifier provisions and their likely impact. And, on the Privacy side of HIPAA, HIPAAdvisors Steve Fox, Esq, and Rachel Wilson, Esq, of Pepper Hamilton, explain how commonly owned health organizations can and may wish to be considered one covered entity for purposes of HIPAA compliance.

Finally, this issue welcomes Bruce Hall as the new Editor of HIPAAlert and Director of Phoenix' Web services. Bruce brings more than 10 years of editorial and web management experience, much within healthcare. We also wish Diane Boettcher -- a terrific web manager! -- success as she moves onward and upward....

D'Arcy Guerin Gue, Publisher
daggue@phoenixhealth.com

==========

2 / H I P A A n e w s

*** Senate Looks at IT Vulnerabilities in Wake of Disaster ***

Not wasting any time, the U.S. Senate Governmental Affairs Committee held a hearing Wednesday in the wake of this week's attacks in New York and Washington to determine whether computer networks that run vital services are vulnerable to terrorism. U.S. officials have been working to organize cooperative information-sharing between critical industrial and service sectors as well as with the National Infrastructure Protection Center. But participation has been limited, in part, by concerns that sensitive private sector data might be publicly released.

For more information, go to:
http://www.hipaadvisory.com/news/index.htm#0912cw

*** Groups Fear for Privacy in Fight Against Terrorists ***

As authorities turned to the Internet in their investigation of this week's terrorist attacks, privacy advocates have expressed fears that antiterrorist measures could end up

jeopardizing the Americans' personal privacy. Cindy Cohn, legal director of the Electronic Frontier Foundation, anticipates that government officials soon will make demands for "everything from increased e-mail surveillance to use of facial recognition systems that could aid authorities to match suspects in public places to a database of criminals." "There are probably some people who will propose extreme measures in the interest of saying that they are doing something," said David Sobel, a lawyer with the Electronic Privacy Information Center in Washington. There were no such proposals coming from Congress on its first day back at work since the attacks, and indeed some lawmakers cautioned against overreacting.

For more information, go to:
http://www.hipaadvisory.com/news/2001/0913wsj.htm

*** Health Industry Voices New Opposition to Transactions Delay ***

In a September 6th letter to Congress, the Coalition for Health Information Policy (CHIP), representing healthcare information associations AHIMA, AMIA, CHIM and HIMSS, wrote "to express opposition to proposals that would delay the compliance deadline for the Transaction Standards regulation, scheduled to be fully effective in October 2002." The letter to Senate Ways and Means Chair William Thomas and House Ways and Means Health subcommittee Chair Nancy Johnson, stated that "the Transactions and Code Sets standards represent an absolutely essential first step toward the standardized exchange of health information and data definitions - a step that can be adequately planned for within the announced implementation timeline, and modified successively as the remaining transaction-related HIPAA rules are released."

To read the full text of the CHIP letter, go to:
http://www.hipaadvisory.com/news/2001/0913chip.htm

*** Privacy Fears May Deter HIV Patients From Treatment ***

According to an August report of AIDS Care, HIV patients are so worried about the confidentiality of their HIV-positive status, that they will actually forgo treatment to prevent the release of this information. Researchers from Duke University studied confidentiality issues of 15 HIV-infected patients, and reported that "the fear of a breach in confidentiality is definitely affecting the care that HIV-infected patients receive. Most study patients experienced or knew someone who had experienced a breach in confidentiality."

For more information, go to:
http://www.hipaadvisory.com/news/2001/0912ac.htm

==========
3 / H I P A A security

*** Assessments and Disaster Recovery Plans - Where to Begin? ***

By Eric Maiwald, CTO,& Barry Lyons, Director Business Development,
Fortrex Technologies

Notwithstanding HIPAA regulations, every hospital should have a definitive enterprise security posture. Hospitals incorporate computer networks, with external ports (Internet connectivity, modems, and other communication ports), which have become important tools to assist in best care practices. The challenge is that these “open systems” also create gaping holes for unwelcome intruders. To facilitate a strong security position and be ready for a potential disaster, hospitals need to take the same steps that the financial community has embraced for years: constant, vigilant enterprise security review along with a solid disaster recovery plan (DRP).

> Security Assessment: First Steps

Vigilant security starts with a Technical Security Assessment -- which has four objectives:

-- Identify the technical requirements for information security
-- Provide a high-level assessment of the technical threats and risks to information
-- Assess effectiveness of existing policies and countermeasures
-- Provide recommendations to improve the information security environment in an efficient and cost effective manner.

When HIPAA is added to this list, one more objective applies:

-- Identify areas of non-compliance with HIPAA regulations

A Technical Security Assessment encompasses both external (public) and internal (private)network access points. The internal assessment examines the organization’s information security posture from the position of a knowledgeable insider. The external assessment examines the organization from the perspective of an outsider. This is the view that a hacker might have if such a person were to target the organization.

The Technical Security Assessment identifies vulnerable points. Once the assessment is completed, all data is analyzed and a report is generated that makes recommendations to minimize the risk. All vulnerabilities (High, Medium and Low)are brought to the organization’s attention with recommended remediation.

"HIGH" vulnerabilities must be addressed immediately. They are found on systems and servers that can be easily and immediately compromised, and if compromised by an unauthorized individual/entity, could seriously hurt an organization's ability to function. Included are systems that could divulge highly sensitive information (including personal health information, or PHI) that could damage not only the organization but also its patients and customers.

Based on the information provided by the assessment, potential damage scenarios are created. For each scenario, recommendations are developed to manage the potential risk. This information is provided in a report, as part of risk identification.

For HIPAA compliance, the assessment team must also analyze the organization against requirements of HIPAA regulations. For each area of non-compliance, a rating is developed to show the extent of non-compliance. Recommendations are developed to assist the organization to become HIPAA compliant. It should be recognized that, irrespective of HIPAA, hospitals and any organization with patient health records or other sensitive information should conduct a Technical Security Assessment. Only then will an organization understand its risks and where they are situated.

> Disaster Recovery Planning: First Steps

Once the assessment is completed, it is likely to reveal several areas that need addressing, including Security Policy Development, Incident Response Plans, Security Awareness Training, 24 x 7 network intrusion monitoring, and alarm reporting. All of these are vitally important, but one major concern, especially for organizations that offer 24 x 7 service, is a well thought out, documented Disaster Recovery Plan (DRP).

Before a DRP is developed, a Requirements Analysis is performed to determine the necessary actions to be performed, internally or with an external entity, for the development of an actual DRP. What this means is that information is gathered, analyzed and then reported in order to define what elements the DRP will have to include. The DRP preparation plan includes four stages:

-- Business Impact Analysis
-- Developing the Disaster Recovery Plan
-- Testing the Disaster Recovery Plan
-- Proposed Project Plan

For each of the first three stages, the current state of a DRP within an organization is identified and recommendations are made for further actions. The proposed project plan then outlines the steps needed to complete the DRP, if required, and estimates the level of effort required.

The most important stage is the Business Impact Analysis, in which an attempt is made to determine the impact on the staff and the business if a particular disaster occurs. (The word “attempt” is used because no one can determine the actual impact of a disaster; each is different in scope and magnitude.) A significant aspect of this phase entails identifying critical applications in all departments, and the maximum amount of time a particular system or service can remain unavailable before an adverse impact is realized. This takes a thorough investigation by qualified, experienced individuals because every factor must be examined, from current network architecture to the history of natural disasters in the organization’s location.

> The Bottom Line: Fundamental Issues

Overall, when it comes to technical security, senior management should be able to answer these questions:

1. Do I have a firm grasp of where my network and other security vulnerabilities are today? Have they been documented?
2. When was the last security assessment performed? Was it documented? Were the “fixes” completed and then re-tested? Were they documented?
3. Can someone outside or inside obtain information that they shouldn’t have? What documentation do I have to confirm this?
4. Do our security protections meet or exceed HIPAA Security Rule requirements? What documentation is available confirming this?
5. What disaster recovery plans do we have for servers, critical applications, patient records? Is the plan documented? Has it been tested? Has it been reviewed by a qualified third party?
6. Are procedures in place to monitor and regularly reassess security? Is there documentation that procedures are followed?

If “don’t know” -- or worse, “no” -- is the answer to even some of these questions, the organization should go to work on a Technical Security Assessment. If the answer to question 5 above from ANY healthcare provider is “no, there isn't a documented disaster recovery plan”, the organization and, perhaps, patient lives are clearly at risk. It is imperative to develop a disaster recovery plan immediately, with the first action item being a Technical Security Assessment.

Eric Maiwald, CISSP, CTO and Barry Lyons, Director of Business Development for Fortrex Technologies, each have over 15 years experience in enterprise networks and technical security. Eric is author of the new book "Network Security: A Beginner's Guide." Fortrex Technologies, a partner of Phoenix Health Systems, is a leading information security services provider, with specialties in HIPAA and healthcare information security.

==========

4 / H I P A A regs

*** National Identifiers: How They Fit into the HIPAA Puzzle ***

by D'Arcy Guerin Gue and Angie Atcher, Phoenix Health Systems
---

> Why Do We Need Unique National Identifiers?

Over the past three decades, the healthcare industry and the Federal government have explored many approaches to arresting double-digit increases in healthcare costs. Strategies have included group insurance plans, subsidized plans, managed care, self-insured funds, wellness programs, and preventative patient education. HCFA introduced Medicare rules limiting allowable charges and requiring standardized transaction processes. Traditional health plans followed suit, introducing cost-saving electronic billing, claims processing, and other business interactions that relied upon computerized coding to identify transactions and parties to the transactions.

Unfortunately, few efforts were made to standardize the elements of what has become an industry-wide movement towards healthcare transactions automation. Today, single providers find themselves with different identifier codes assigned by different health plans,and even within the same health plans. The same identifier may be issued to multiple providers. Millions of employers -- often the sponsors of health plans -- are subject to similar inconsistencies, along with health plans and patients themselves. Employers, providers, payors, clearinghouses, patients and vendors -- all participants in healthcare transactions -- must contend with the unnecessary confusion, extra work, processing delays, and high costs created by this lack of standardization.

Healthcare claims are often delayed or rejected due to processing errors and incorrect coding formats -- including incorrect identifier codes for parties to transactions. Many Americans have experienced the frustration of being caught in the middle when employers, health plans and providers are unable to coordinate eligibility and claims processes because of missing or erroneous data. Some have experienced how non-standard identifiers have contributed to unethical electronic billing practices and other fraud and abuse both in Medicare and in the private health sector. For many providers, the problems created by lack of standards has been a major reason for refusing to submit claims electronically, despite the potential cost advantages.

In the early 1990’s, healthcare industry leaders, DHHS and Congress became increasingly concerned about the costly lack of

standardization in the “business” of healthcare. These concerns precipitated Congress’ decision to include “administrative simplification” provisions in HIPAA, requiring that healthcare transactions and identifiers for employers, health plans, providers and individuals be standardized nationally.

> Who and What Are Covered?

Section 1173 of HIPAA Administrative Simplification called for “a standard unique health identifier for each individual, employer, health plan, and health care provider for use in the healthcare system.” The Act recognized that DHHS would have “to take into account multiple uses for identifiers and multiple locations and specialty classifications for healthcare providers.” The proposed rules apply to health plans and clearinghouses, and any provider electronically transmitting any of the transactions covered by HIPAA. As a practical matter, software vendors that have contracts with health plans and providers to support healthcare transactions will also be affected by the identifier requirements.

“Electronic transmissions” includes all media, including magnetic tape, disk, CD media, the Internet, extranets, leased lines, dial-up lines, and private networks. Telephone voice response, "faxback" systems, and HTML interaction are not included. Transmissions within a corporate entity are not affected.

> What is the Current Status of National Identifiers?

Two rules have been proposed (NPRMs), thus far:

-- National Provider Identifier, published May 7, 1998
-- National Employer Identifier, published June 16, 1998

The National Health Plan Identifier and the National Health Identifier for Individuals have not yet been proposed. DHHS has indicated that it will develop an identifier for health plans before the end of 2001, to aid in administration of benefits and to improve the transmission of healthcare transactions.

Development of an identifier for individuals has been postponed indefinitely, and its future is uncertain. Despite the positives of the individual identifier concept, it has generated much public and advocacy group controversy regarding how it can be implemented without compromising individual privacy.

> How Are Identifiers Chosen?

The selection of standard identifiers is no small task. Since standards for identifiers do not exist, DHHS has consulted extensively with designated health industry standards maintenance organizations (DSMOs), including the Workgroup for Electronic Data

Interchange (WEDI), the National Uniform Billing Committee (NUBC), the National Uniform Claim Committee (NUCC) and the American Dental Association (ADA) to develop proposed standards. “Guiding Principles for Standards Selection,” which are detailed in HIPAA, were used by the implementation teams to set proposed identifier standards.

> The National Provider Identifier:

-- What Is It?

Presently, health plans assign an identifying number to each provider with whom they conduct electronic business. Since providers typically work with several health plans, they are likely to have a different identifier number for each plan. The standard Provider Identifier (NPI) will ensure that each provider has one unique identifier to be used in transactions with all health plans. National Provider Identifiers must be used by all providers, and accepted by all clearinghouses and health plans in connection with the electronic transactions that are covered by HIPAA.

The original, proposed format for the NPI was an eight digit alphanumeric identifier. However, the healthcare industry has widely criticized this format, claiming that major information systems incompatibilities will make it too expensive and difficult to implement. DHHS has now revised its recommendation, stating that the final rule will specify a 10-position numeric identifier with a check digit in the last position to help detect keying errors. The NPI is expected to carry no intelligence; in other words, its characters will not in themselves provide information about the provider. Each healthcare provider will receive just one unique identifier which will remain with the provider throughout its (his/her) life as a provider.

> How Will We Implement the NPI?

DHHS has recommended that the NPI be implemented through a central electronic National Provider System (NPS), to be managed by HCFA. The NPS will consist of a combination of existing Federal health plans, Medicaid state agencies and a new, Federally-directed registry -- all of whom will assign identifiers, or “enumerate” providers. Federal health plans and Medicaid agencies will enumerate their own healthcare providers. Providers who don’t belong to one of the included Federal programs will be enumerated by the Federally-directed registry.

NPI enumeration will be implemented in phases. First, providers that submit electronic Medicare transactions will automatically be assigned an NPI. Non-Medicare health plans such as Medicaid and HMOs will then phase in enumeration of their providers. Providers using these programs will not need to apply for an NPI, but will have to decide which health plan will provide it. Providers who do not participate in any Federal health plans or Medicaid but who

transmit standard HIPAA transactions electronically, will have to apply directly to the new Federal registry for their NPIs. Finally, providers who don't participate in any Federal plans or transmit the electronic transactions covered by HIPAA are expected to be enumerated after all other providers. The NPS will maintain the national database in perpetuity.

Implementation of the NPI is likely to be a challenge, both for the Federal government and the healthcare community. The proposed National Provider System does not yet exist, and while enlisting the participation of Federal plans may help lower set-up costs, coordinating an initial nation-wide enumeration process and managing the transition from multiple identifiers to a single identifier environment may become complicated. Providers and other organizations will have to update their legacy information systems, administrative processes, reference files and forms in order to ensure continuity between old provider identifiers and the new NPIs. Some providers and vendors will find that their systems require tweaking or significant reengineering to accommodate the new standard. Health plans, clearinghouses and software vendors may have to perform software conversions to meet the requirement.

> The National Employer Identifier (NEI):

-- What Is It?

Because employers are primary sponsors of health plans, they often must be identified within healthcare transactions. DHHS has recommended that the National Employer Identifier be the number currently assigned to employers by the Internal Revenue Service.

The IRS Employer Identification Number (EIN) is a 9-digit number (xx-xxxxxx) that is already used as the employer identifier for enrollment/disenrollment in a health plan, health claim, eligibility, and premium payment. As the EIN is a publicly available number that does not reference any individual, it is unlikely to create any privacy issues. DHHS also has emphasized that it does not enable access to tax information.

-- How Will We Implement the NPI?

Implementation of the National Employer Identifier is expected to have a much milder impact than implementation of the Provider Identifier. The EIN is already in wide use, so few entities will be required to make substantial process changes. Nevertheless, all providers, payors, and clearinghouses currently using other employer identifiers in electronic transactions will be required to convert to the EIN. Employers will need to disclose their EIN when requested. Some payors and clearinghouses may need to alter their systems to accommodate the new standard.

> What Will Be the Benefits of National Identifiers?

Standardization of transaction data elements - including the codes that identify parties to healthcare transactions -- is expected to help reduce healthcare fraud, transaction errors, redundant administrative efforts and, ultimately, costs. Many hope that standardized healthcare transactions processes ("administrative simplification")combined with adequate privacy and security protections, will provide a foundation for an efficient, streamlined nation-wide healthcare information infrastructure.

Clearly, initial costs of implementation will overshadow any early benefits. Significant benefits are likely to be realized only over the next several years as fewer referrals are denied or rejected for erroneous provider identifiers, and the healthcare delivery environment becomes increasingly streamlined, standardized and cost-effective.

To review the full text of the proposed National Provider and Employer Identifier Rules, go to:
http://www.hipaadvisory.com/regs/index.htm

D'Arcy Guerin Gue is Executive Vice President, Knowledge Services and Business Development, of Phoenix Health Systems. Angie Atcher is a Director of Phoenix Health Systems, and a senior member of its HIPAA Solutions Team.
==========

5 / H I P A A d v i s o r : Can Your Organization Qualify as an "Affiliated Covered Entity?"

by Steve Fox, Esq, and Rachel Wilson, Esq, Pepper Hamilton LLP

QUESTION: Our company owns a large national chain of outpatient and residential mental health facilities. Is each of these facilities individually responsible for the notifications and consents required under the privacy rule? With the exception of an on-site clinic for employees, no protected health information is created, used or disclosed at our corporate headquarters. Is there a way to implement an enterprise-wide HIPAA compliance initiative? Each of our facilities is a separate and distinct corporate entity. Does that make a difference?

ANSWER: Legally separate and distinct covered entities may designate themselves as a single covered entity for the purpose of complying with the privacy rule (the "rule") as long as the entities are "affiliated," meaning they share common ownership or control. "Common ownership" is defined as an ownership or equity interest of five percent (5%) or more. "Common control"

exists if an entity has the power, directly or indirectly, to significantly influence or direct the actions or policies of another entity. The covered entities that together make up an "affiliated covered entity" are subject to separate liability under the rule.

Affiliated organizations don't have to share similar functions or activities in order to designate themselves as a single covered entity. If your company decided to designate all of its facilities as a single affiliated covered entity for the purpose of HIPAA compliance, the on-site clinic at the company's headquarters could be included as part of that affiliated covered entity.

Perhaps the biggest advantage to this designation is the potential cost savings benefit to larger organizations. Affiliated covered entities may utilize a single shared notice of privacy practices for the entire enterprise, promulgate one consent form, designate one privacy official, and implement one set of privacy policies and procedures. However, it's important to remember that this consolidation does not extend to the restrictions on the use and disclosure of protected health information (PHI) under the rule. If an affiliated covered entity performs more than one type of covered function, each individual component of the affiliated covered entity must still comply with those provisions of the rule that are specifically applicable to its covered functions. For example, if one of the components of an affiliated covered entity is a health care provider with a direct treatment relationship, that component entity would still be required to obtain a consent prior to using or disclosing PHI; even if such use or disclosure was between another component of the affiliated covered entity.

In situations where a covered entity (such as the on-site health clinic in the example above) is part of a larger organization that is not itself regulated by HIPAA, then only the healthcare component of the larger organization must comply with HIPAA. The organization as a whole is referred to as a "hybrid entity" under the rule, since only part of it must be HIPAA compliant. Any use or disclosure of PHI by the health care component of the hybrid entity is subject to the privacy standards even when such use or disclosure is made internally within the hybrid entity. Moreover, the health care components of hybrid entities are required to implement firewalls or safeguards between itself and the larger hybrid identity in order to insure meaningful privacy protection.

To read past HIPAAdvisor articles, go to:
http://www.hipaadvisory.com/action/HIPAAdvisor.htm

Steve Fox, Esq, is a partner at the Washington, D.C. office of Pepper Hamilton LLP. This article was co-authored by Rachel H.

Wilson, Esq, an associate at Pepper Hamilton LLP.
http://www.pepperlaw.com/

Disclaimer: This information is general in nature and should
not be relied upon as legal advice.

==========

Hot HIPAAlert news! Phoenix Health Systems is now offering an
HTML version of HIPAAlert. To switch to this new, cutting
edge HTML format, just fill out the short form at:
http://www.hipaadvisory.com/signup/change.cfm

==========
Don't miss --
>>> SECURELY HIPAA! Our Fall Audioconference Series <<<

Sept 26 -- Understanding & Managing Security Assessments
Oct 17 -- Security Implementation for the Non-Technical Manager
-- With Eric Maiwald, CISSP, CTO, of Fortrex Technologies and
Tom Grove, Director, Phoenix Health Systems

For more info, or to enroll, go to:
http://www.hipaadvisory.com/ezcart/enter.cfm

Other outstanding HIPAA Audioconferences and tapes available at:
http://www.hipaadvisory.com/ezcart/

==========

BRING YOUR HIPAA QUESTIONS AND IDEAS TO LIFE AT...H I P A A l i v e!

Join 3600 other thinkers, planners, learners and lurkers
who are already members of our sister e-mail discussion list.
We almost make HIPAA fun! Almost.

Subscribe now at: http://www.hipaadvisory.com/live/

==========

RAISE YOUR ORGANIZATION'S HIPAAWARENESS WITH H I P A A n o t e s !

Nearly 7000 industry members are already receiving a weekly byte
of HIPAA. Your HIPAAnote is suitable for publishing on your
organization's intranet or newsletter & comes free to your e-mailbox.
Subscribe now at: http://www.hipaadvisory.com/notes/

==========
COMMENTS? Email us at info@phoenixhealth.com
SUBSCRIBE? Visit http://www.hipaadvisory.com/alert/
ARCHIVES: http://www.hipaadvisory.com/alert/newsarchives.htm
==========

==========

FORWARD this posting to interested associates, who may subscribe free to HIPAAlert at:
http://www.hipaadvisory.com/alert/
Subscribe to our free discussion list at:
http://www.hipaadvisory.com/live/
Get a weekly byte of HIPAA at:
http://www.hipaadvisory.com/notes/
Switch to HTML version or to text version at:
http://www.hipaadvisory.com/signup/change.cfm

You are currently subscribed to hipaalert as:kmckinst@dmhhq.state.ca.us
To unsubscribe send a blank email to leave-hipaalert-8507990O@lists.hipaalert.com